

Annual 47 C.F.R. § 64.2009(e) CPNI Certification

EB Docket 06-36

Annual 64.2009(e) CPNI Certification for 2010

Date filed: January 28, 2011

Name of company covered by this certification: Equivoice, Inc.

Form 499 Filer ID: 822086

Name of signatory: Richard Pierce

Title of signatory: Vice President

I, Richard Pierce, certify that I am an officer of the company named above, and acting as an agent of the company, that I have personal knowledge that the company has established operating procedures that are adequate to ensure compliance with the Commission's CPNI rules. *See 47 C.F.R. § 64.2001 et seq.*

Attached to this certification is an accompanying statement explaining how the company's procedures ensure that the company is in compliance with the requirements set forth in section 64.2001 *et seq.* of the Commission's rules.

The company has not taken any actions (proceedings instituted or petitions filed by the company at state commissions, the court system, or the Commission against data brokers) during the period covered by this certification.

The company has not received any customer complaints during the period covered by this certification concerning the unauthorized release of CPNI.

Signed 
Richard Pierce

Annual 47 C.F.R. § 64.2009(e) CPNI Certification

EB Docket 06-36

Attachment 1: Statement Concerning Company Procedures

General duty, training, and discipline.

Equivoice, Inc. (the "Company") has adopted and distributed to all employees a confidentiality policy that addresses proper handling and use of CPNI and advises all employees of their duty to safeguard CPNI. Employees are advised that violations of the confidentiality policy will subject an employee to disciplinary action, up to and including immediate termination of employment. The Company makes CPNI available to employees only on a need-to-know basis.

Use of customer proprietary network information without customer approval (47 C.F.R. § 64.2005); Approval required for use of customer proprietary network information (47 C.F.R. § 64.2007); Notice required for use of customer proprietary network information (47 C.F.R. § 64.2008); Safeguards required for use of customer proprietary network information (47 C.F.R. § 64.2009)

The Company does not use, disclose, or permit access to CPNI for marketing purposes. The Company does not disclose CPNI to third parties or permit third parties to access or use CPNI.

Safeguards on the disclosure of customer proprietary network information (47 C.F.R. § 64.2010)

The Company does not provide any telephone or in-store access to CPNI. Customers requesting CPNI by telephone will be provided with CPNI only by sending it to the customer's address of record or by calling the customer at the telephone address of record.

Customers may access their CPNI online only after they have been authenticated without using readily available biographical information or account information. After initial authentication, customers may only access CPNI online by providing a password that is not prompted by a request for readily available biographical information or account information. Customers that have lost or forgotten their passwords may retrieve their passwords by proving an answer to a shared secret question. If a customer cannot provide the correct password or the correct response to the shared secret question, the customer must be reauthenticated and must establish a new password.

The Company notifies customers immediately by email to the customer's email address of record or by voicemail to the telephone number of record of any changes to customer password, answer to shared secret questions, online account information, or address of record. This notice does not reveal the changed information and is sent to the existing

address or telephone number of record, not to an address or telephone number that has been changed.

Notification of customer proprietary information security breaches (47 C.F.R. § 64.2011)

The Company's operating procedures require notification of relevant law enforcement agencies and customers in accordance with FCC rules in the event of a breach of CPNI. The Company maintains records of any breaches discovered, notifications made to law enforcement, and notifications made to customers. These records include, where available, dates of discovery and notification, a detailed description of the CPNI that was the subject of the breach, and the circumstances of the breach. The Company retains these records for 2 years.